IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

SAVEITSAFE, LLC,	§	
	§	
Plaintiff,	§	
	§	CIVIL ACTION NO. 6:20-cv-00286
v.	§	
	§	
ORACLE CORPORATION,	§	**JURY TRIAL DEMANDED**
	§	
Defendant.	§	

ORIGINAL COMPLAINT

Plaintiff SaveItSafe, LLC ("Plaintiff" or "SaveItSafe"), by and through its attorneys, for its Original Complaint against Oracle Corporation ("Defendant" or "Oracle"), and demanding trial by jury, hereby alleges as follows:

I. NATURE OF THE ACTION

1. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 271, *et seq.*, to enjoin and obtain damages resulting from Defendant's unauthorized use, sale, and offer to sell in the United States of products, methods, processes, services and/or systems that infringe SaveItSafe's United States patent, as described herein.

2. Oracle manufactures, provides, uses, sells, offers for sale, imports, and/or distributes infringing products and services; and encourages others to use its products and services in an infringing manner, including their customers, as set forth herein.

3. SaveItSafe seeks past and future damages and prejudgment and post-judgment interest for Oracle's past infringement of the Patent-in-Suit, as defined below.

II. PARTIES

4. Plaintiff SaveItSafe is a limited liability company organized and existing under the laws of the State of Delaware with its principal place of business located at 1312 Sunset Court, Tool, Texas, 75143. SaveItSafe's registered agent for service of process in Texas is Corporation Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701.

5. SaveItSafe is the result of a corporate spin off from No Magic, Inc. ("No Magic"). No Magic was established in 1996 by the current CEO of SaveItSafe (who was also the CEO of No Magic) and his brother, the inventor of the Patent-in-Suit. No Magic primarily focused on software development. It garnered substantial success, generating over 10,000 customer companies, including those in the energy, automotive, financial, logistics, telecommunications and space exploration (NASA) industries. No Magic's commercial success led to its eventual acquisition by a world leader in engineering software, Dassault Systèmes SE ("Dassault"). However, the rights to the Patent-in-Suit were not sold to Dassault as part of its acquisition of No Magic, but were instead transferred to SaveItSafe so that SaveItSafe's CEO and the inventor of the Patent-in-Suit could maintain ownership and control.

6. On information and belief, Defendant Oracle is a corporation organized under the laws of the State of Delaware with established places of business in this District at 2300 Oracle Way, Austin, Texas 78741; 5300 Riata Park Court, Building B, Austin, Texas, 78727; and 613 NW Loop 410, Suite 1000, San Antonio, Texas 78216. Oracle's registered agent for service of process in Texas is Corporation Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701.

III. JURISDICTION AND VENUE

7. This is an action for patent infringement which arises under the Patent Laws of the United States, namely, 35 U.S.C. §§ 271, 281, 283, 284 and 285.

8. This Court has exclusive jurisdiction over the subject matter of this action under 28 U.S.C. §§ 1331 and 1338(a).

9. On information and belief, venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b), 1391(c), and 1400(b) because Oracle has regular and established places of business in this District, transacted business in this District, and has committed and/or induced acts of patent infringement in this district.

10. On information and belief, Defendant Oracle is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

IV. FACTUAL ALLEGATIONS

PATENT-IN-SUIT

11. SaveItSafe is the owner of all right, title and interest in and to U.S. Patent No. 8,929,552 (the "'552 Patent"), entitled "Electronic Information and Cryptographic Key Management System" issued on January 6, 2015. The '552 Patent discloses improved systems and methods for securing electronic information. The information that is to be secured is associated with a cryptographic key and that key is then also secured by encrypting it, saving it, restricting access to it, or by other means. A key management system may be tasked with securing the key and confirming that the key is indeed secured. The claimed invention of the '552 Patent was intended to address problems with conventional methods of securing electronic information: conventional systems and methods failed to secure all of the components of a cryptosystem and did not adequately address securement of cryptographic keys. '552 Patent, 5:1-7:3. The '552 Patent

addressed these shortcomings, in one respect, by enabling a function of the system only after it has first confirmed, via a second functionality that is independent of the functionality that secured the key, that the relevant cryptographic key has been secured. *Id*. at 7:19-23. Examples of the functions that can be enabled in response to the confirmation of the securement of the key include enabling the encryption of electronic information, decryption of electronic information, transfer of electronic information, saving of electronic information, reading of electronic information, rewriting electronic information, creating electronic information, and manipulating electronic information. Additionally, the ’552 Patent discloses enhanced security measures such as using secure socket layer for transferring keys or information and requiring simultaneous access requests from multiple administrators in order to allow access to secure electronic information. A true and correct copy of the ’552 Patent is attached as **Exhibit A.**

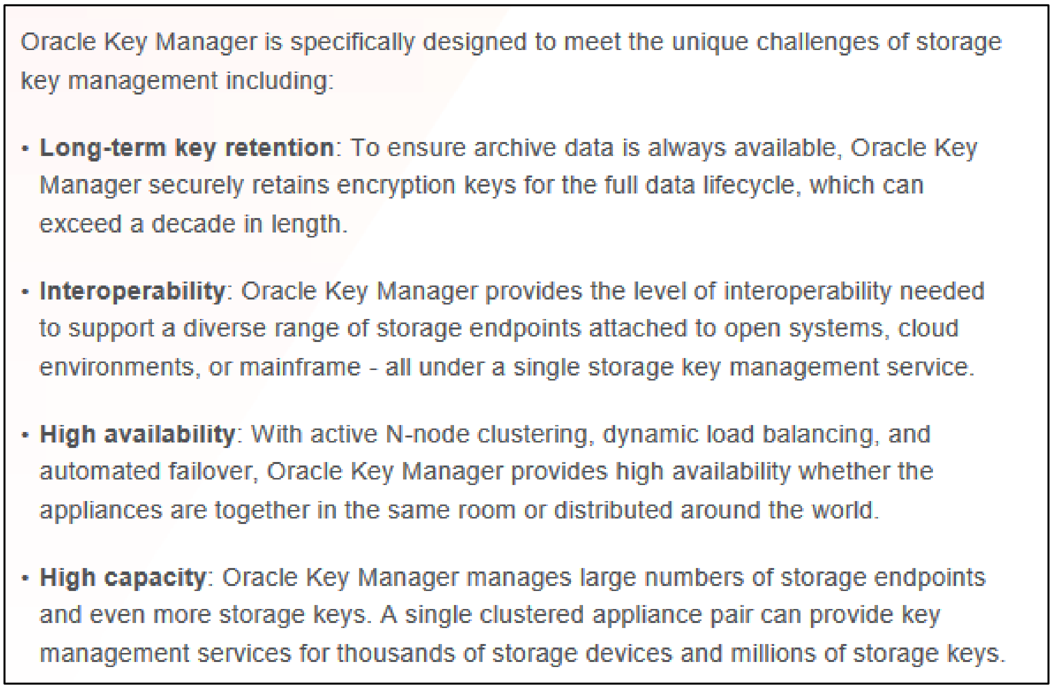
12. SaveItSafe is the assignee of the ’552 Patent and has all rights to sue for infringement and collect past and future damages for the infringement thereof.

DEFENDANT’S ACTS

13. Oracle is a global provider of secure communication and encryption products and solutions. Specifically, Oracle provides hardware, software, and services that secure electronic information via key management and data security systems to its customers in the United States, including in this District. For example, Oracle’s Key Manager (“OKM”) and Key Vault (“OKV”) provide transaction security, key storage, and key security. Oracle describes its OKM as “a comprehensive key management system designed to address the rapidly growing enterprise commitment to storage-based data encryption.” Oracle Key Manager Overview, November 2018, page 5, available at: https://www.oracle.com/technetwork/articles/systems-hardware-architecture/o10-013-st-ckm-solution-4-187263.pdf. Similarly, the OKV is described as “simplif[ying] the deployment of encryption across the enterprise with extremely scalable,

continuously available key management." Oracle Key Vault Datasheet, page 1, available at: https://www.oracle.com/a/devo/docs/dbsec/okv/ds-security-key-vault-18-2019-05-08.pdf.

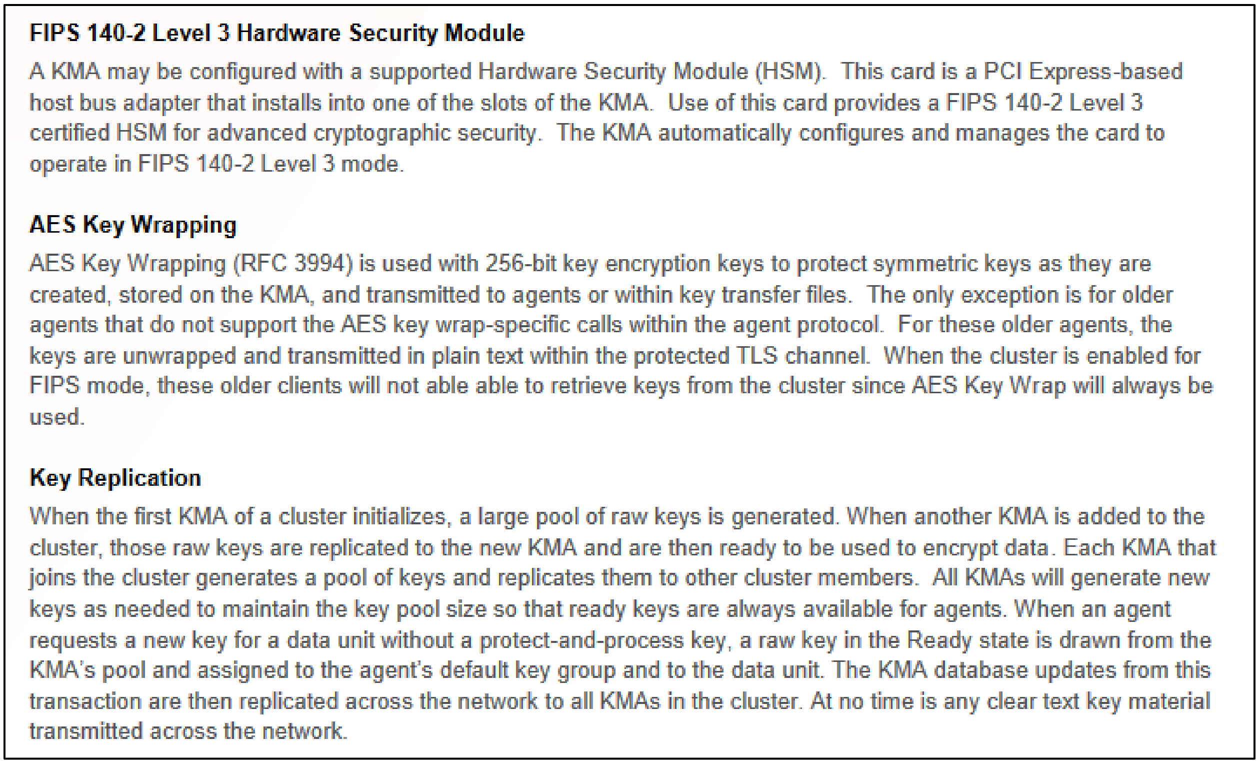
14. Oracle's centralized key management products and solutions associate a cryptographic key with secured information. This cryptographic key is further secured by encryption or other technical means. Once the securement of the cryptographic key is confirmed, the key management systems may enable subsequent cryptographic or data processing functions based on that confirmation. For example, the relevant high-level functions of Oracle's OKM and OKV are illustrated in the excerpts below from Oracle's documentation:



Oracle Key Manager is specifically designed to meet the unique challenges of storage key management including:

- **Long-term key retention**: To ensure archive data is always available, Oracle Key Manager securely retains encryption keys for the full data lifecycle, which can exceed a decade in length.
- **Interoperability**: Oracle Key Manager provides the level of interoperability needed to support a diverse range of storage endpoints attached to open systems, cloud environments, or mainframe - all under a single storage key management service.
- **High availability**: With active N-node clustering, dynamic load balancing, and automated failover, Oracle Key Manager provides high availability whether the appliances are together in the same room or distributed around the world.
- **High capacity**: Oracle Key Manager manages large numbers of storage endpoints and even more storage keys. A single clustered appliance pair can provide key management services for thousands of storage devices and millions of storage keys.

Oracle Key Manager Overview, November 2018, page 5, available at: https://www.oracle.com/technetwork/articles/systems-hardware-architecture/o10-013-st-ckm-solution-4-187263.pdf



FIPS 140-2 Level 3 Hardware Security Module

A KMA may be configured with a supported Hardware Security Module (HSM). This card is a PCI Express-based host bus adapter that installs into one of the slots of the KMA. Use of this card provides a FIPS 140-2 Level 3 certified HSM for advanced cryptographic security. The KMA automatically configures and manages the card to operate in FIPS 140-2 Level 3 mode.

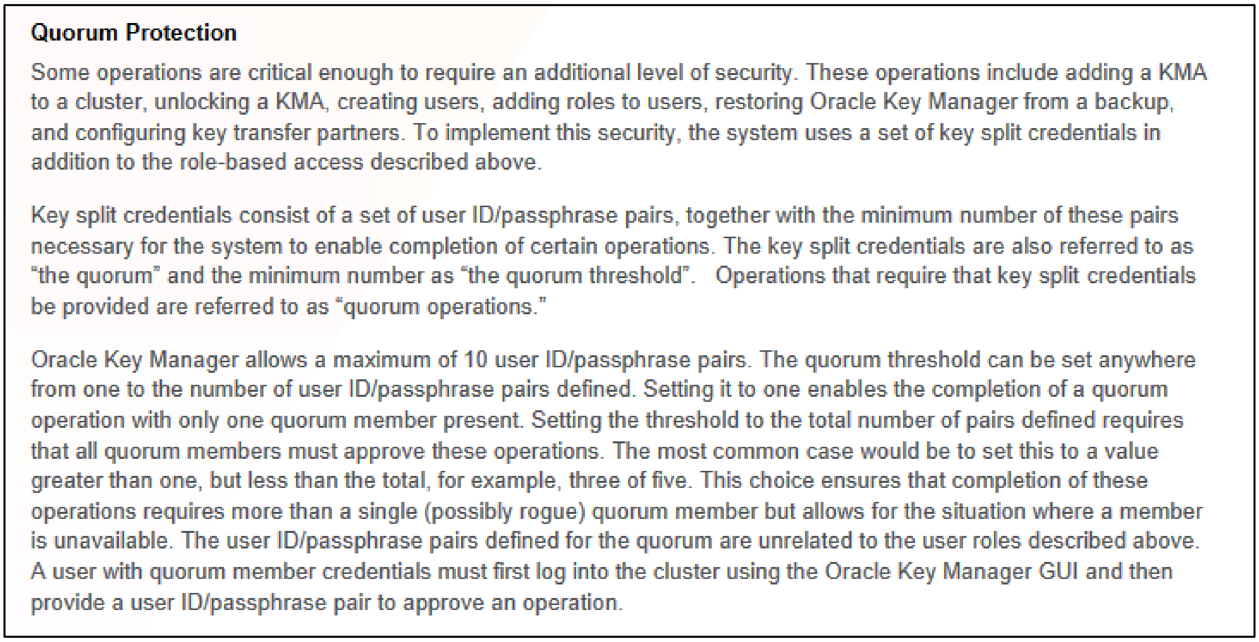
AES Key Wrapping

AES Key Wrapping (RFC 3994) is used with 256-bit key encryption keys to protect symmetric keys as they are created, stored on the KMA, and transmitted to agents or within key transfer files. The only exception is for older agents that do not support the AES key wrap-specific calls within the agent protocol. For these older agents, the keys are unwrapped and transmitted in plain text within the protected TLS channel. When the cluster is enabled for FIPS mode, these older clients will not able able to retrieve keys from the cluster since AES Key Wrap will always be used.

Key Replication

When the first KMA of a cluster initializes, a large pool of raw keys is generated. When another KMA is added to the cluster, those raw keys are replicated to the new KMA and are then ready to be used to encrypt data. Each KMA that joins the cluster generates a pool of keys and replicates them to other cluster members. All KMAs will generate new keys as needed to maintain the key pool size so that ready keys are always available for agents. When an agent requests a new key for a data unit without a protect-and-process key, a raw key in the Ready state is drawn from the KMA's pool and assigned to the agent's default key group and to the data unit. The KMA database updates from this transaction are then replicated across the network to all KMAs in the cluster. At no time is any clear text key material transmitted across the network.

Id. at 18.



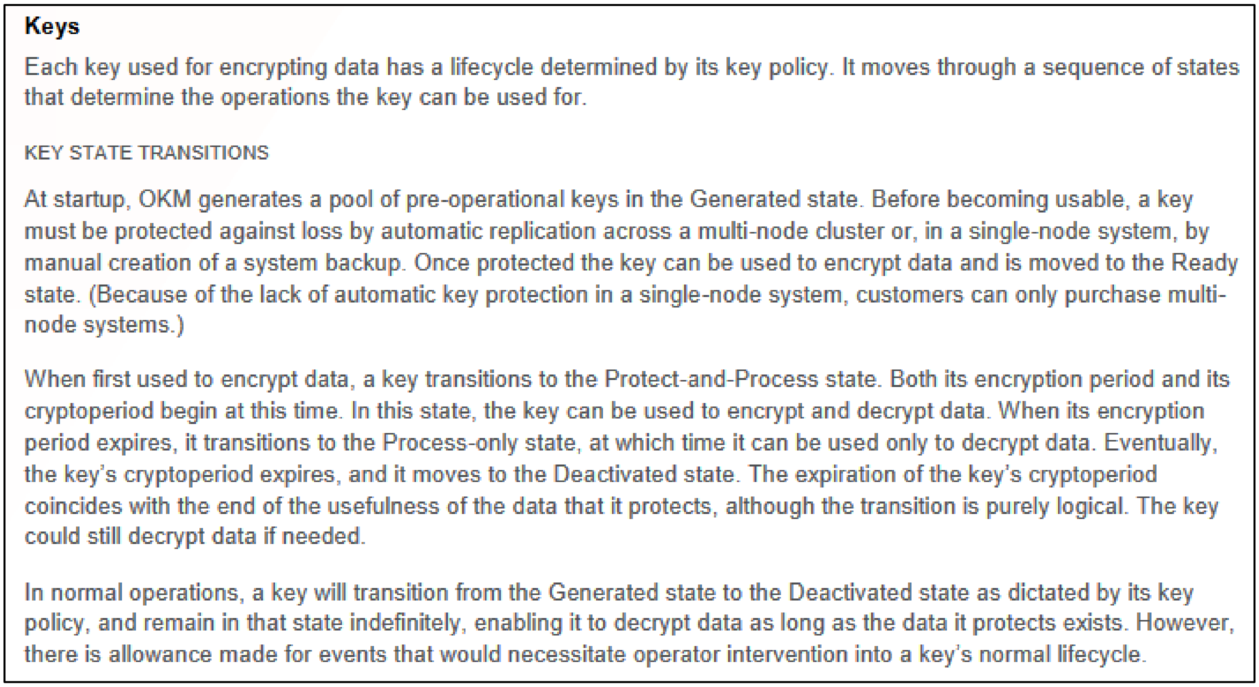
Quorum Protection

Some operations are critical enough to require an additional level of security. These operations include adding a KMA to a cluster, unlocking a KMA, creating users, adding roles to users, restoring Oracle Key Manager from a backup, and configuring key transfer partners. To implement this security, the system uses a set of key split credentials in addition to the role-based access described above.

Key split credentials consist of a set of user ID/passphrase pairs, together with the minimum number of these pairs necessary for the system to enable completion of certain operations. The key split credentials are also referred to as "the quorum" and the minimum number as "the quorum threshold". Operations that require that key split credentials be provided are referred to as "quorum operations."

Oracle Key Manager allows a maximum of 10 user ID/passphrase pairs. The quorum threshold can be set anywhere from one to the number of user ID/passphrase pairs defined. Setting it to one enables the completion of a quorum operation with only one quorum member present. Setting the threshold to the total number of pairs defined requires that all quorum members must approve these operations. The most common case would be to set this to a value greater than one, but less than the total, for example, three of five. This choice ensures that completion of these operations requires more than a single (possibly rogue) quorum member but allows for the situation where a member is unavailable. The user ID/passphrase pairs defined for the quorum are unrelated to the user roles described above. A user with quorum member credentials must first log into the cluster using the Oracle Key Manager GUI and then provide a user ID/passphrase pair to approve an operation.

Id. at 19.



Keys

Each key used for encrypting data has a lifecycle determined by its key policy. It moves through a sequence of states that determine the operations the key can be used for.

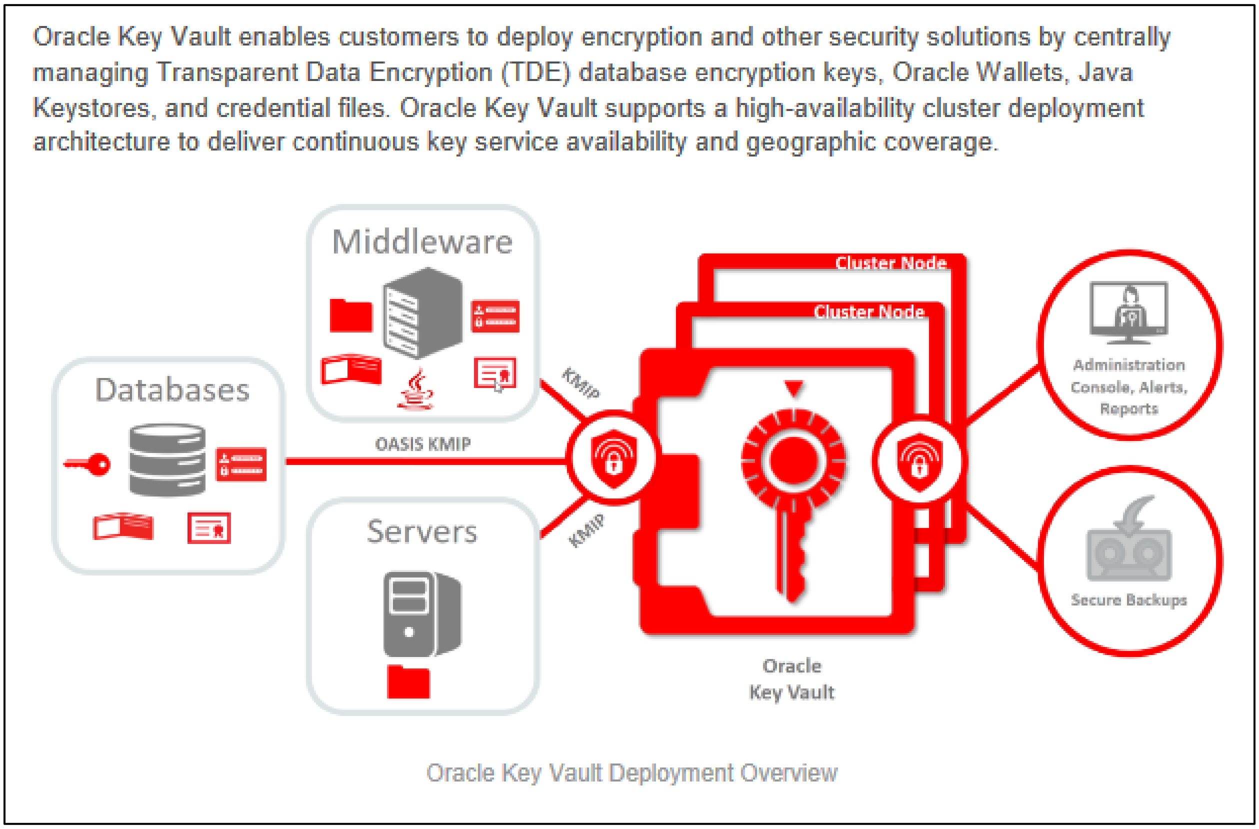
KEY STATE TRANSITIONS

At startup, OKM generates a pool of pre-operational keys in the Generated state. Before becoming usable, a key must be protected against loss by automatic replication across a multi-node cluster or, in a single-node system, by manual creation of a system backup. Once protected the key can be used to encrypt data and is moved to the Ready state. (Because of the lack of automatic key protection in a single-node system, customers can only purchase multi-node systems.)

When first used to encrypt data, a key transitions to the Protect-and-Process state. Both its encryption period and its cryptoperiod begin at this time. In this state, the key can be used to encrypt and decrypt data. When its encryption period expires, it transitions to the Process-only state, at which time it can be used only to decrypt data. Eventually, the key's cryptoperiod expires, and it moves to the Deactivated state. The expiration of the key's cryptoperiod coincides with the end of the usefulness of the data that it protects, although the transition is purely logical. The key could still decrypt data if needed.

In normal operations, a key will transition from the Generated state to the Deactivated state as dictated by its key policy, and remain in that state indefinitely, enabling it to decrypt data as long as the data it protects exists. However, there is allowance made for events that would necessitate operator intervention into a key's normal lifecycle.

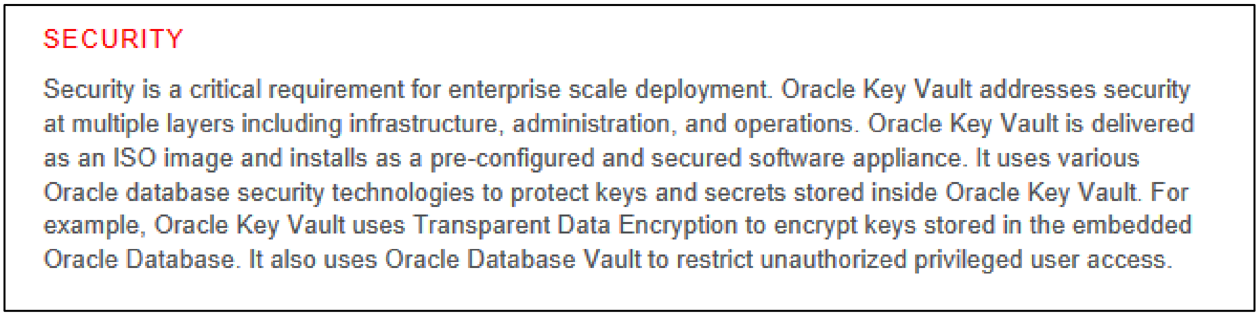
Id. at 13.



Oracle Key Vault enables customers to deploy encryption and other security solutions by centrally managing Transparent Data Encryption (TDE) database encryption keys, Oracle Wallets, Java Keystores, and credential files. Oracle Key Vault supports a high-availability cluster deployment architecture to deliver continuous key service availability and geographic coverage.

Oracle Key Vault Deployment Overview

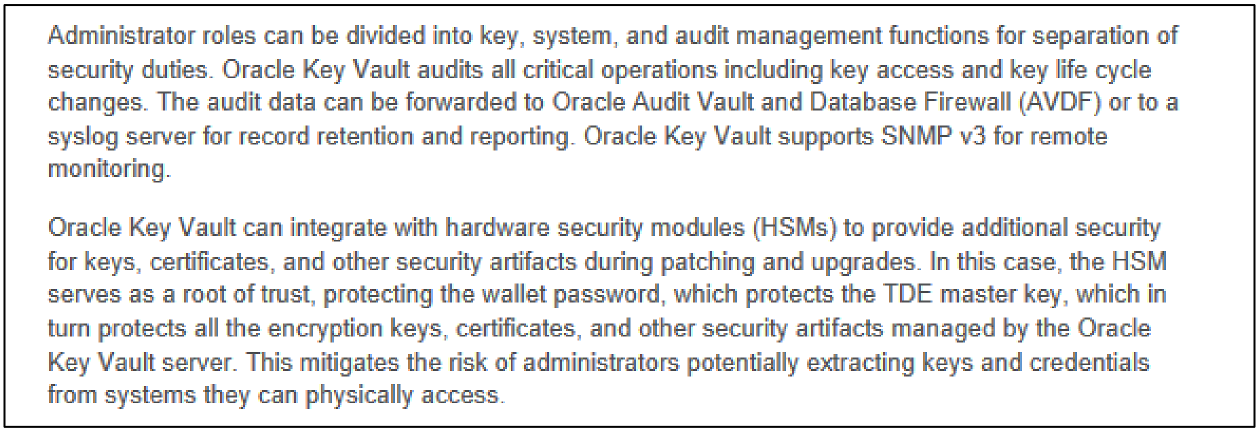
Oracle Key Vault Datasheet, page 1, available at: https://www.oracle.com/a/devo/docs/dbsec/okv/ds-security-key-vault-18-2019-05-08.pdf.



SECURITY

Security is a critical requirement for enterprise scale deployment. Oracle Key Vault addresses security at multiple layers including infrastructure, administration, and operations. Oracle Key Vault is delivered as an ISO image and installs as a pre-configured and secured software appliance. It uses various Oracle database security technologies to protect keys and secrets stored inside Oracle Key Vault. For example, Oracle Key Vault uses Transparent Data Encryption to encrypt keys stored in the embedded Oracle Database. It also uses Oracle Database Vault to restrict unauthorized privileged user access.

Id. at 3.



Administrator roles can be divided into key, system, and audit management functions for separation of security duties. Oracle Key Vault audits all critical operations including key access and key life cycle changes. The audit data can be forwarded to Oracle Audit Vault and Database Firewall (AVDF) or to a syslog server for record retention and reporting. Oracle Key Vault supports SNMP v3 for remote monitoring.

Oracle Key Vault can integrate with hardware security modules (HSMs) to provide additional security for keys, certificates, and other security artifacts during patching and upgrades. In this case, the HSM serves as a root of trust, protecting the wallet password, which protects the TDE master key, which in turn protects all the encryption keys, certificates, and other security artifacts managed by the Oracle Key Vault server. This mitigates the risk of administrators potentially extracting keys and credentials from systems they can physically access.

Id. at 4.

15. Oracle instructs its customers regarding the implementation and operation of the accused instrumentalities, including detailed instructions for the OKV (e.g. at https://docs.oracle.com/en/database/oracle/key-vault/index.html) and OKM (e.g. https://docs.oracle.com/en/storage/storage-software/oracle-key-manager/index.html.)

16. On information of belief, Defendant Oracle also implements contractual protections in the form of license and use restrictions with its customers to preclude the unauthorized reproduction, distribution and modification of its software.

17. Moreover, on information and belief, Defendant Oracle implements technical precautions to attempt to thwart customers who would circumvent the intended operation of Oracle's products.

18. Oracle had knowledge of the ’552 Patent and its infringing conduct as early as the date when SaveItSafe effected service of its Original Complaint.

V. COUNTS OF PATENT INFRINGEMENT

COUNT ONE
INFRINGEMENT OF U.S. PATENT NO. 8,929,552

19. SaveItSafe incorporates by reference its allegations in the preceding paragraphs as if fully restated in this paragraph.

20. SaveItSafe is the assignee and owner of all right, title and interest to the ’552 Patent. SaveItSafe has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

21. On information and belief, Defendant Oracle, without authorization or license from SaveItSafe, has been and is presently directly infringing at least claim 4 of the ’552 Patent, as infringement is defined by 35 U.S.C. § 271(a), including through making, using (including for testing purposes), selling and offering for sale methods and articles infringing one or more claims of the ’552 Patent. Defendant Oracle is thus liable for direct infringement of the ’552 Patent pursuant to 35 U.S.C. § 271(a).

22. Exemplary infringing products include Oracle’s Key Manager and Key Vault which support securing electronic information and a cryptographic key by using one function to secure the key, a second function to confirm the securing, enabling a function in response to that confirmation, and restricting access to electronic information to situations where the system receives substantially simultaneous access requests.

23. On information and belief, Defendant Oracle, without authorization or license from SaveItSafe, has been and is presently indirectly infringing at least claim 4 of the ’552 Patent, including actively inducing infringement of the ’552 Patent under 35 U.S.C. § 271(b). Such

inducements include without limitation, with specific intent to encourage the infringement, knowingly inducing consumers to use infringing articles and methods that Oracle knows or should know infringe one or more claims of the ’552 Patent. Oracle instructs its customers to make and use the patented inventions of the ’552 Patent by operating Oracle’s products in accordance with Oracle’s specifications. Oracle specifically intends its customers to infringe by implementing its key management systems to secure electronic information and a cryptographic key by using one function to secure the key, a second function to confirm the securing, enabling a function in response to that confirmation, and restricting access to electronic information to situations where the system receives substantially simultaneous access requests, as set forth above.

24. On information and belief, Defendant Oracle, without authorization or license from SaveItSafe, has been and is presently indirectly infringing at least claim 4 of the ’552 Patent, including contributory infringement of the ’552 Patent under 35 U.S.C. § 271(c) and/or § 271(f), either literally and/or under the doctrine of equivalents, by selling, offering for sale, and/or importing into the United States, the infringing products. Oracle knows that the infringing products (i) constitute a material part of the inventions claimed in the ’552 Patent; (ii) are especially made or adapted to infringe the ’552 Patent; (iii) are not staple articles or commodities of commerce suitable for non-infringing use; and (iv) are components used for or in its key management systems to secure electronic information and a cryptographic key with a first and second function and restrict access to electronic information in an infringing manner.

25. As a result of Oracle’s infringement of the ’552 Patent, SaveItSafe has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such infringement under 35 U.S.C. § 284, but in no event, less than a reasonable royalty.

VI. JURY DEMAND

26. Plaintiff SaveItSafe demands a trial by jury of all matters to which it is entitled to trial by jury, pursuant to FED. R. CIV. P. 38.

VII. PRAYER FOR RELIEF

WHEREFORE, SaveItSafe prays for judgment and seeks relief against Defendant as follows:

A. That the Court determine that one or more claims of the Patent-in-Suit is infringed by Defendant Oracle, either literally or under the doctrine of equivalents;

B. That the Court award damages adequate to compensate SaveItSafe for the patent infringement that has occurred, together with prejudgment and post-judgment interest and costs, and an ongoing royalty for continued infringement;

C. That the Court award enhanced damages pursuant to 35 U.S.C. §284; and

D. That the Court award such other relief to SaveItSafe as the Court deems just and proper.

DATED: April 13, 2020

Respectfully submitted,

/s/ Andrew G. DiNovo
Andrew G. DiNovo
Texas State Bar No. 00790594
adinovo@dinovoprice.com
Daniel L. Schmid
Texas State Bar No. 24093118
dschmid@dinovoprice.com
DINOVO PRICE LLP
7000 N. MoPac Expressway, Suite 350
Austin, Texas 78731
Telephone: (512) 539-2626
Telecopier: (512) 539-2627

Counsel for Plaintiff SaveItSafe, LLC